SPYWOLF

Security Audit Report

Completed on

February 25, 2023

OVERVIEW

This audit has been prepared for **NERO** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

NERO

PROJECT DESCRIPTION

According to their whitepaper:

"Nero protocol uses nonlinear adaptive control theory to automagically output optimal borrow rates. Furthermore, all risk parameters—base rate, close factor, LTV threshold, liquidation penalty, and others—are dynamically calculated based on the composition of your collateralised debt position."

Release Date: Presale starts in February, 2023

Category: Finance

CONTRACT INFO

Token Name
Nero

Symbol
NPT

Contract Address
0x23F9a46A2c06f5249702aAd1b9B1Fd1b6e6833CF

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Feb 21, 2023

Verified?
Yes

Total Supply
100,000,000,000

Status
Not launched

TAXES

Buy Tax
none

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	99999999999.99998 NPT
Median Transfer Amount	99999999999.99998 NPT
Average Transfer Amount	99999999999.99998 NPT
First transfer date	2023-02-21
Last transfer date	2023-02-21
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-02-21 20:42:03 UTC
Created	2023-02-21 20:42:03 UTC
Create TX	0x42412a82ff7cbd3449551ea0786318436adcf8492c707ab066b37946dcdd38d1
Creator	0x60b9c3bd8405e2b46ac13f7b450d8865dc449b52

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

High Risk

No high risk-level threats found in this contract.

FOUND THREATS

⚠ Medium Risk

Owner can add address to frontRunnerList.
Addresses included in the frontRunnerList will be subject to taxes different from sell taxes (default 98%).
This can lead to inability to sell for addresses added in the frontRunnerList.

This measure is taken to protect the project from malicious users activity during launch, based on project's owner criteria and explanation.

```
function setFrontRunner(address[] memory accounts) public onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        if (!frontRunnerList[accounts[i]]) {
            frontRunnerList[accounts[i]] = true;
        }
    }
}

function _transfer(
    address sender,
    address recipient,
    uint256 amount
) internal override virtual {
.................
if (isFrontRunner(sender) || isFrontRunner(recipient)) {
    if (recipient == pairAddr) {
        tax = baseUnit * (frontFee > 0 ? frontFee : 98);
    }
}
.................
}

function isFrontRunner(address account) public view returns (bool) {
    return frontRunnerList[account];
}
```

- Recommendation:
  - Consider automatic mechanism with certain criteria for adding addresses in frontRunnerList instead of manual one.
    Example: Sanction every address that try to buy and sell in the same block or in 1-2 blocks distance (few seconds).

FOUND THREATS

⚠ Medium Risk

Owner can set sell fee up to 5% and front fee up to 100%.
If address is added to frontRunList front fee will apply instead.
Combined buy+sell=5%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold or transferred.
Most of the tokens do not apply transfer fees, but if they do this, will be described in the information above.

This measure is taken to protect the project from malicious users activity during launch, based on project's owner criteria and explanation.

```
uint256 public constant feeLimit = 5;

function setFees(uint256 _sellFee, uint256 _frontFee) public onlyOwner {
    require(_sellFee <= feeLimit, "ERC20: sell tax higher than tax limit");
    sellFee = _sellFee;
    frontFee = _frontFee;
}
```

- Recommendation:
  - Considered as a good tax deduction practice to have buy and sell fees combined not exceed 25%.

FOUND THREATS

Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function setExcluded(address[] memory  accounts) public onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        if (!excludedList[accounts[i]]) {
            excludedList[accounts[i]] = true;
        }
    }
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

NERO

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner cannot set a transaction limit

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

*No tokenomics found at the time of the audit.

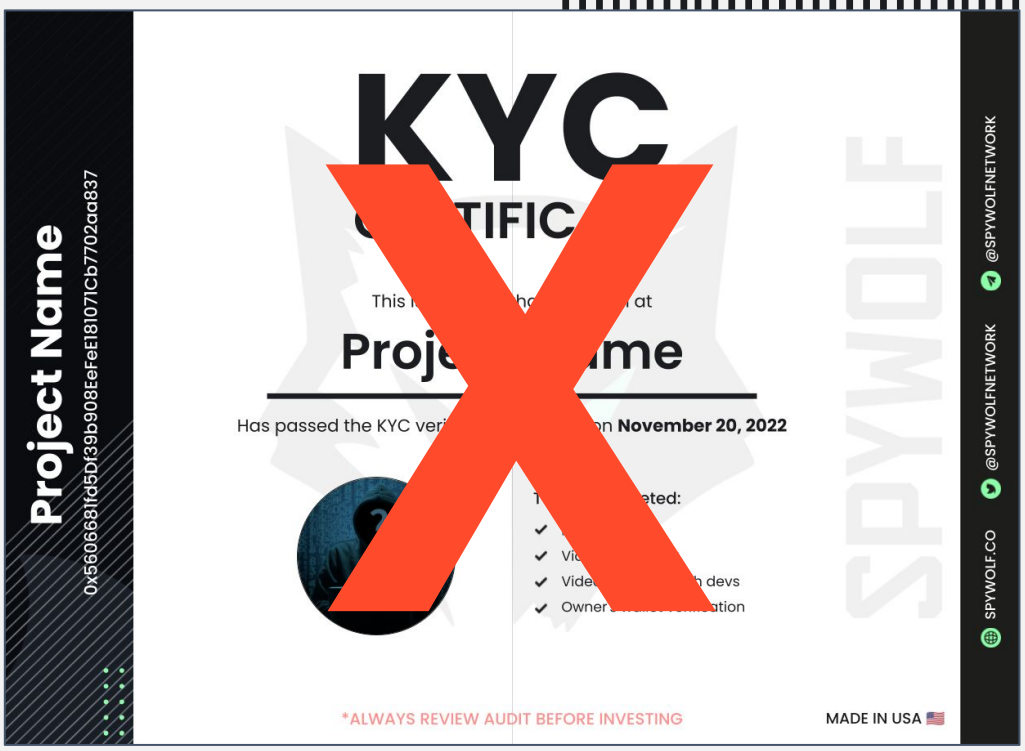
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://neroprotocol.com/

Domain Registry
whois.rrpproxy.net

Domain Expiration
2024-02-14

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

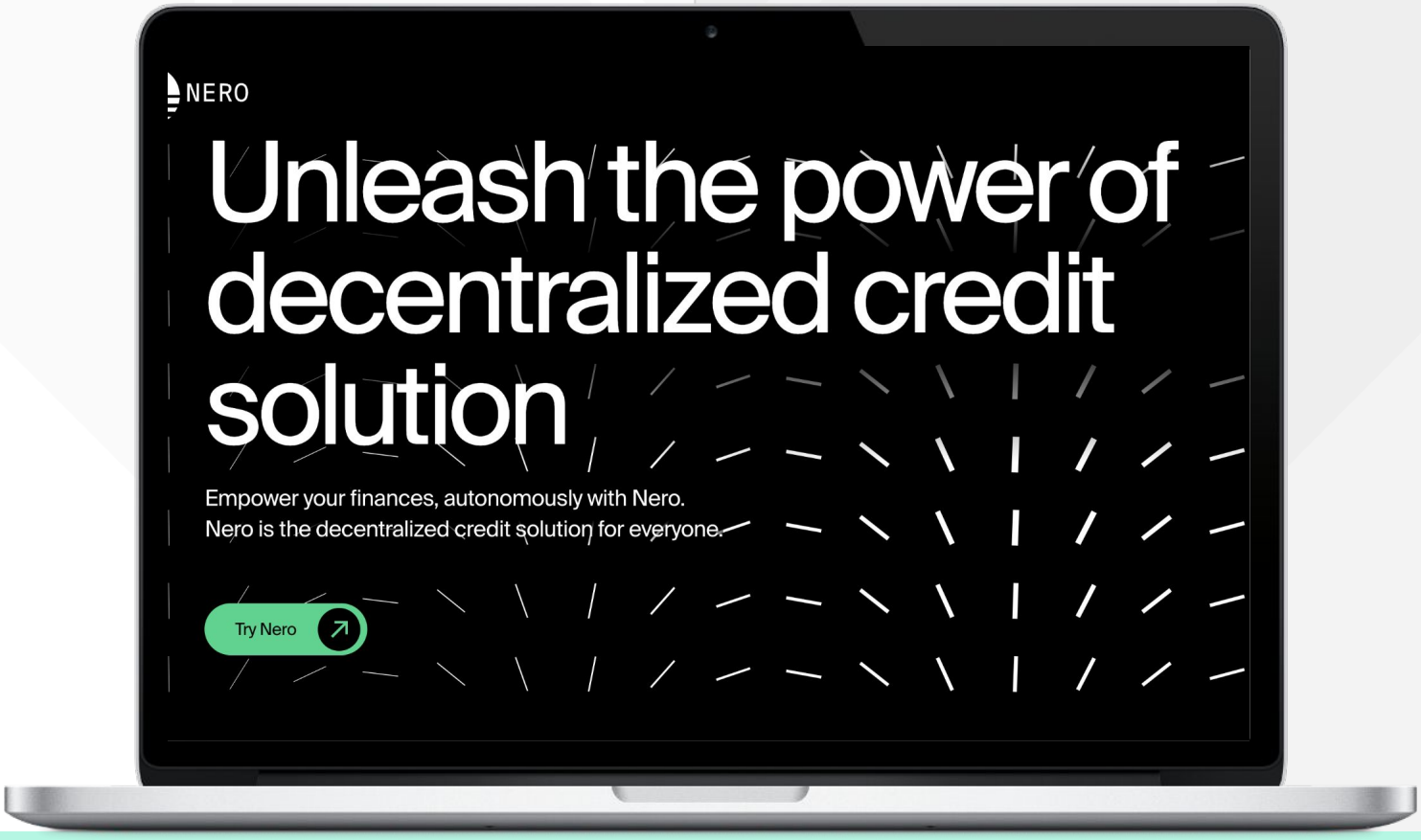
Design
Really nice design and color scheme. Very interactive and attractive for the users.

Content
The information helps new investors understand what the product does right away. No grammar errors found. .

Whitepaper
Well written but a bit short

Roadmap
Yes

Mobile-friendly?
Yes



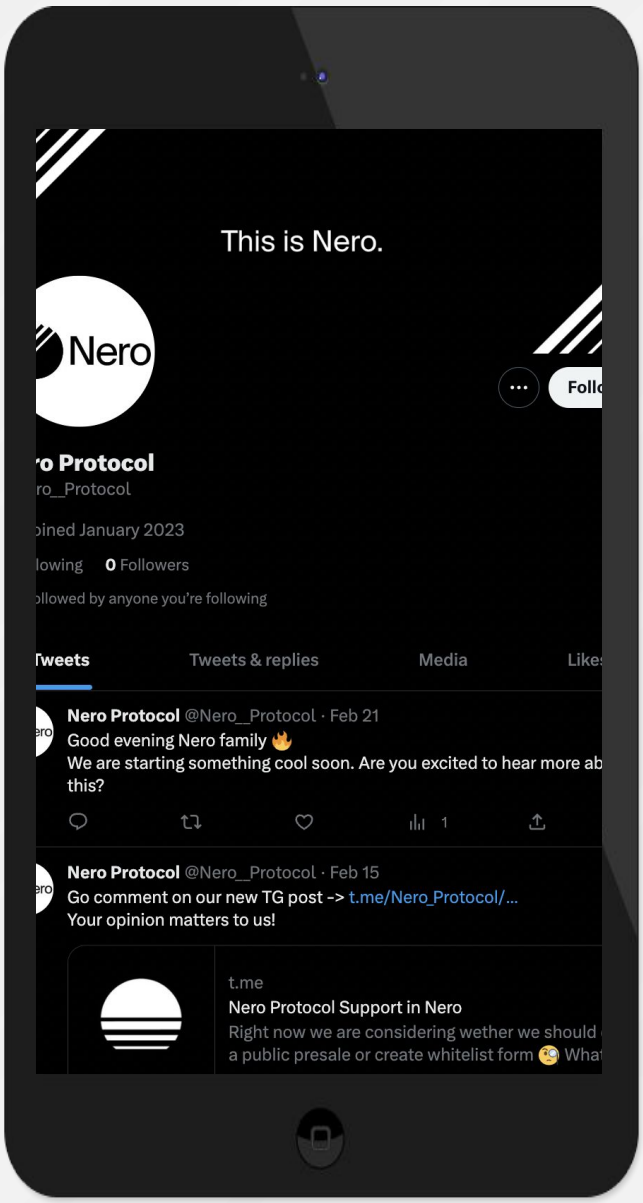
neroprotocol.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Social media pages are brand new.



Twitter

@Nero__Protocol

- @Nero__Protocol

Discord

- Not available

Telegram

@Nero_Protoco

- 1500 members
- Active mods and devs

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 400 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.